REMARKS

Upon entry of this amendment, claims 1, 3-5, 7-18, 20-23, 29, 31, and 46-50 will be pending. By this amendment, claims 6, 24-26 and 28 have been canceled; and claims 1, 3-5, 7-13, 18, 20-23, 29, 31, and 46-50 have been amended. No new matter has been added.

§112 Rejection of Claims 1, 3-18, 20-26, 28, 29, 31 and 46-50

In Section 5 of the office action dated June 1, 2010 ("the Office Action"), claims 1, 3-18, 20-26, 28, 29, 31 and 46-50 stand rejected under 35 U.S.C. 112, first paragraph for failing to comply with the written description requirement.

Relevant claims have been amended to address the rejection.

Accordingly, it is submitted that the rejection of claims 1, 3-18, 20-26, 28, 29, 31 and 46-50 based upon 35 U.S.C. §112 has been overcome by the present remarks and withdrawal thereof is respectfully requested.

§103 Rejection of Claims 1, 3-6, 8, 9, 18, 20-21, 26, 28-29 and 46-49

In Section 7 of the Office Action, claims 1, 3-6, 8, 9, 18, 20-21, 26, 28-29 and 46-49 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Steenkamp *et al.* (U.S. Patent Publication No. 2004/0168184; hereinafter referred to as "Steenkamp").

Regarding amended claim 1, it now recites:

> A method of adding a client as a member of a hub network, comprising:

(a) detecting a client connected to a server in a hub network;

(b) authenticating the client to determine an identify of the client;

(c) authorizing the client to determine that <u>the client is a compliant device that operates according to rules defined for the hub network</u>;

(d) adding the client as a member in the hub network <u>when it is determined that the client has been detected, authenticated, authorized, and is in a local environment of the server</u>; and

(e) providing licenses for content data bound to the hub network to members of the hub network,

(f) wherein <u>a source version of the content data is stored on the server, and copies of the source versions are stored on the compliant device as sub-copy versions.</u>

(emphasis / limitation designations added)

In addition to the arguments presented in responses to previous office actions (which are maintained here), following additional arguments are presented.

Regarding newly-add limitations in (c), (d), and (f), they now recite "authorizing the client to determine that the client is a compliant device that operates according to rules defined for the hub network; adding the client as a member in the hub network when it is determined that the client has been detected, authenticated, authorized, and is in a local environment of the server; ... wherein a source version of the content data is stored on the server, and copies of the source versions are stored on the compliant device as sub-copy versions."

These limitations, as well as limitations for claims 3-5 and 7-17, are disclosed in

at least Paragraphs [0030], [0032], [0081], [0086]-[0087], [0090], and [0107] (of the

Publication of the present application – Pub. No. 2004/0117484) as follows (emphasis

added):

> [0030] ... <u>Before adding a device as a member to the hub network HN1, the PVR 105 authenticates a device, confirming the identity of the device, and authorizes an authenticated device, confirming that the device is a compliant device</u>. If the PVR 105 does not authenticate and authorize a device, the PVR 105 does not add that device to the hub network HN1. ...

> [0032] ... The <u>locked content data stored by the server is the source for copies of the content data in the hub network and is the "source version." Copies of the source version content data are stored on clients and are "sub-copy versions"</u> ...

> [0081] After successfully authenticating the client device, the server receives an add request to add the client device from a user, block 1820. The server waits to proceed with adding a client device until the server receives an affirmative request from a user to add a specific client device. In another implementation, the server requests approval or confirmation from the user to add an authenticated device when the device is detected instead of waiting for a request from the user. In another implementation, the server waits to authenticate the client device until after receiving a request or approval to add the client.

> [0086] In an alternative implementation, a server automatically attempts to add detected client devices upon detection, or uses a <u>set of rules to determine when to attempt to add connected client devices</u>. In another implementation, the server automatically attempts to authenticate and authorize detected client devices, but does not add an authenticated and authorized device as a member until after receiving a user request or approval.

> [0087] In another implementation, <u>when the device count has reached the device limit and the server is attempting to</u>

add another device, the server contacts a device registration server, such as through an external network connection.- The device registration server indicates whether the client device is to be added to the hub network or not. The device registration server maintains information for hub networks and their member devices. The device registration server can use various criteria to determine whether to allow the client device to be added or not. In one implementation, the device registration server compares a threshold to how many hub networks to which the client device has already been added as a member. In another implementation, the device registration server compares the number of devices already added to the hub network to a second device limit, allowing the client device to be added if the device count is below the second device limit. ...

[0090] The server disables the licenses for sub-copy versions of bound instances bound to the server's hub network for the client device to be removed, block 1910. The server sends a disable request to the client indicating the sub-copy versions to be disabled and the client disables the corresponding licenses. In addition, the removed client device will not be able to receive a new license or be able to refresh an existing license for a bound instance bound to the hub network from which the client device was removed. In one implementation, a compliant client device automatically disables all licenses for sub-copy versions stored on the client and for bound instances bound to the hub network from which the client has been removed once the client has been removed. Removing a client from one hub network does not necessarily disable licenses for sub-copy versions for bound instances bound to another hub network.

[0107] ... In one implementation, a server can revoke a key if the server has determined the key has been compromised. In this case the server requests compliant devices disable the revoked key so that the revoked key will not be used to access secure media content.

In addressing the limitations of claim 1, as well as other claims, the Office Action

cites Steenkamp, Paragraphs 60, 65, 68, 98, and 102, where "licenses are granted (issued)

only to clients who have been added as members (subscribers) of the digital rights

network. Further, these paragraphs seem to refer to terms such as content distributor,

authenticate, and licenses. These paragraphs of Steenkamp are recited here for reference

(emphasis added):

> [0060] Each of the content distributors 20 caches content
> received from multiple content providers 16, and thus
> assists with the temporary storage of content near the
> "edges" of a network so as to reduce network congestion
> that would otherwise occur were a content provider 16 to
> distribute content responsive to every content request
> received from a content consumer. Each content distributor
> 20 is equipped to respond to requests received via the
> network 18 from the multiple content destinations 22 (e.g.,
> subscribers or other types of content consumers) within a
> specified service area or conforming to specific criteria.
> Specifically, a content distributor 20, after performing the
> necessary authorization and verification procedures, may
> forward content that it has cached to a content destination
> 22 or, if such content has not been cached, may issue a
> request for the relevant content to a content provider 16.
> For example, if the content comprises a live "broadcast",
> the content may be directly forwarded via the content
> distributor 20 to the content destination 22.

> [0065] The exemplary content distributor 20 is shown to
> host a local content server 40 and a digital rights agent 28.
> Alternatively, the digital rights agent 28 may be located
> remotely from the content distributor 20, and accessed by
> the content distributor 20 via the network 18. The local
> content server 40 may again be a streaming media server
> that streams cached (or freshly received) media. The digital
> rights agent 28 operates to provide intelligent content and
> revenue security to content providers 16 by processing
> access and revenue criteria, personalizing content for
> delivery to a content destination 22, and personalizing and
> managing key delivery to a content destination 22. Broadly,
> the digital rights agent 28 operates securely to authenticate
> a content destination 22 (e.g., utilizing secure tokens and
> X.509 certificates), securely to retrieve and cache product
> key information and content rights (e.g., access criteria),

and to forward processed transactions to a commerce service provider 42 (e.g., a CRM operator) that provides billing and clearance services. For example, a digital rights agent 28 may evaluate a content request, received at the content distributor 20 from a content destination 22, based on access criteria specified by a content provider 16, local date and time information, and user credentials and authentication. If a content destination 22 is authorized and/or payment is cleared, requested content might optionally be decrypted, personally watermarked, personally re-encrypted and delivered to the content destination 22.

[0068] To review, the content distribution system 10 is implemented by a distributed collection of digital rights servers 36, digital rights agents 28, and digital rights clients 48 that operate in conjunction with media servers and viewing devices (e.g., players) to protected the rights of a content provider 16 in specific content, while facilitating the widespread distribution of content. A digital rights server 36 enables the content provider 16 to encrypt and associate access criteria (e.g., pay-per-view, pay-per-time, subscription) with content. The digital rights server 36 also manages subscriptions and provides monitoring and statistic tools to a content provider 16. A digital rights agent 28 is a cryptographic component that insures that content rights (e.g., access criteria), as defined by content providers 16, are enforced. Digital rights agents 28 are located within a distribution network (e.g., at an edge server) and validate subscriber content requests against, for example, content access criteria, local date and time, and subscriber credentials. A digital rights client 48 is located at a destination device (e.g., the PC, a STB, and mobile phone, game console or the like) and manages an interface between a secure device 46 and a subscriber.

[0098] A digital rights agent 28 also operates to create licenses for distribution to a content destination 22 so as to allow a content consumer to access specific content. Licenses for content may be created within the digital rights agent 28 utilizing a variety of license formats, based on the relevant user secure media player 46. In some cases, content may be delivered in the clear, but access to the content limited through a simple access control (i.e.,

content is not delivered from a content distributor 20 until
user rights of a content consumer to access the content have
been cleared).

[0102] The content destination 22 (e.g., a secure device 46
operated by a content consumer) is shown to request and
receive licenses from a digital rights agent 28. In one
embodiment, the digital rights agent 28 issues a license on
behalf of a content rights owner (e.g., a content provider
16), and a commerce service provider 42 (e.g., a CRM
operator) for a content consumer. The license is issued if an
access policy associated with the requested content is
satisfied, and the content consumer's account is in order.
Such a license typically contains a content decryption key,
and certain rules governing the use of the decryption key.
The content destination 22 is also shown to receive content
from the content distributor 20, this content typically being
encrypted and requiring the above-mentioned content
decryption key for access.

However, these paragraphs fail to teach or suggest the limitations as recited in

amended claim 1, as well as other claims dependent from claim 1. For example, none of

the cited paragraphs specifically teach or suggest "authorizing the client to determine that

the client is a compliant device that operates according to rules defined for the hub

network". Further, the cited paragraphs fail to teach or suggest "adding the client as a

member in the hub network when it is determined that the client has been detected,

authenticated, authorized, and is in a local environment of the server". Further, the cited

paragraphs fail to teach or suggest "wherein a source version of the content data is stored

on the server, and copies of the source versions are stored on the compliant device as sub-

copy versions".

Based on the foregoing discussions, claim 1, and its dependent claims 3-5 and 7-

17, should be allowable over Steenkamp. Regarding independent claims 18, 29, and 46,

similar arguments as those of claim 1 apply to these claims. Therefore, claims 18, 29, and 46 should also be allowable over Steenkamp. Since claims 20-21 and 47-49 depend from one of claims 18, 29, and 46, claims 20-21 and 47-49 should also be allowable over Steenkamp. Claims 6, 26 and 28 have been canceled.

Accordingly, it is submitted that the rejection of claims 1, 3-6, 8, 9, 18, 20-21, 26, 28-29 and 46-49 based upon 35 U.S.C. §103(a) has been overcome by the present remarks and withdrawal thereof is respectfully requested.

§103 Rejection of Claims 7 and 22

In Section 24 of the Office Action, claims 7 and 22 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Steenkamp, as applied to claims 1 and 18 above, and further in view of Kamperman (U.S. Patent Publication No. 2005/0273608).

The arguments presented in responses to previous office actions are maintained here, and following additional arguments are presented.

Based on the above discussions regarding claims 1 and 18, since claims 7 and 22 depend from claims 1 and 18, claims 7 and 22 should also be allowable over Steenkamp.

Further, amended claim 7 now recites:

> The method of claim 1, wherein determining that the client
> is a compliant device comprises
>
> sending a compliance confirmation request to the client to
> request information from the client to confirm that the
> client will abide by the rules defined for a hub network.

Amended claim 22 now recites:

The method of claim 18, wherein said compliance information indicates that the <u>compliant device will not decrypt locked content data without a license that is bound to a hub network of which the compliant device is a member</u>.

The Office Action states that Kamperman discloses authenticating the client including sending a compliance confirmation request to the client ..." in Paragraphs 5, 6, 29-31, which are recited here:

[0005] One way of protecting content in the form of digital data is to ensure that content will only be transferred between devices if

[0006] the receiving device has been authenticated as being a compliant device,

[0029] In an embodiment the common secret has been shared before performing the distance measurement, the sharing being performed by the steps of,

[0030] performing an authentication check from the first communication device on the second communication device by checking whether said second communication device is compliant with a set of predefined compliance rules,

[0031] if the second communication device is compliant, sharing said common secret by transmitting said secret to the second communication device.

However, none of these paragraphs teach or suggest "sending a compliance confirmation request to the client to request information from the client to confirm that the client will abide by the rules defined for a hub network" or "wherein said compliance information indicates that the ." These paragraphs of kamperman merely recite "performing an authentication check from the first communication device on the second communication device by checking whether said second communication device is

11374848355US1214926.02

compliant with a set of predefined compliance rules."

Accordingly, it is submitted that the rejection of claims 7 and 22 based upon 35 U.S.C. §103(a) has been overcome by the present remarks and withdrawal thereof is respectfully requested.

§103 Rejection of Claims 10, 23, 28, and 31

In Section 27 of the Office Action, claims 10, 23, 28, and 31 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Steenkamp, as applied to claims 9, 18, 26, and 29 above, and further in view of Fransdonk (U.S. Patent Publication No. 2003/0167392).

The arguments presented in responses to previous office actions are maintained here, and following additional arguments are presented.

Further, claims 10, 23, and 31 have been significantly amended. Accordingly, Fransdonk fails to teach or suggest the limitations recited in these claims.

Based on the foregoing discussions, claims 10, 23, and 31 should be allowable over the combination of Steenkamp and Fransdonk. Claim 28 has been canceled.

Accordingly, it is submitted that the rejection of claims 10, 23, 28, and 31 based upon 35 U.S.C. §103(a) has been overcome by the present remarks and withdrawal thereof is respectfully requested.

§103 Rejection of Claims 11, 12 and 50

In Section 32 of the Office Action, claims 11, 12 and 50 stand rejected under 35

U.S.C. 103(a) as being unpatentable over Steenkamp, as applied to claims 9 and 49 above, and further in view of Uhlik (U.S. Patent Publication No. 2007/0112948).

The arguments presented in responses to previous office actions are maintained here, and following additional arguments are presented.

Further, claims 11, 12, and 50 have been significantly amended. Accordingly, Uhlik fails to teach or suggest the limitations recited in these claims.

Based on the foregoing discussions, claims 11, 12, and 50 should be allowable over the combination of Steenkamp and Uhlik.

Accordingly, it is submitted that the rejection of claims 11, 12 and 50 based upon 35 U.S.C. §103(a) has been overcome by the present remarks and withdrawal thereof is respectfully requested.

§103 Rejection of Claims 13 and 25

In Section 38 of the Office Action, claims 13 and 25 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Steenkamp, as applied to claims 1 and 18 above, and further in view of McCann et al. (U.S. Patent No. 7,376,840; hereinafter referred to as "McCann").

The arguments presented in responses to previous office actions are maintained here, and following additional arguments are presented.

Further, claim 13 has been significantly amended. Accordingly, McCann fails to teach or suggest the limitation recited in this claim.

Based on the foregoing discussions, claim 13 should be allowable over the

combination of Steenkamp and McCann. Claim 25 has been canceled.

Accordingly, it is submitted that the rejection of claims 13 and 25 based upon 35 U.S.C. §103(a) has been overcome by the present remarks and withdrawal thereof is respectfully requested.

§103 Rejection of Claims 14-17

In Section 41 of the Office Action, claims 14-17 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Steenkamp, as applied to claim 1 above, and further in view of Abburi *et al.* (U.S. Patent No. 7,203,966; hereinafter referred to as "Abburi").

The arguments presented in responses to previous office actions are maintained here.

Based on the discussions made in the previous office actions, claims 14-17 should be allowable over the combination of Steenkamp and Abburi.

Accordingly, it is submitted that the rejection of claims 14-17 based upon 35 U.S.C. §103(a) has been overcome by the present remarks and withdrawal thereof is respectfully requested.
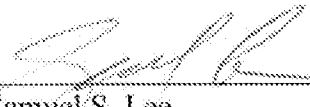
Conclusion

In view of the foregoing, applicants respectfully request reconsideration of claims 1, 3-5, 7-18, 20-23, 29, 31, and 46-50 in view of the remarks and submit that all pending claims are presently in condition for allowance.

In the event that additional cooperation in this case may be helpful to complete its prosecution, the Examiner is cordially invited to contact Applicant's representative at the telephone number written below.

Respectfully submitted,

Dated: _10 - 1 - 10_   By: _____

Samuel S. Lee
Reg. No. 42,791

Procopio, Cory, Hargreaves & Savitch LLP
525 B Street, Suite 2200
San Diego, California 92101-4469
(619) 525-3821